| NODIS Library | Organization and Administration(1000s) | Search |

NASA Procedural Requirements

NPR 1660.1C
Effective Date: May 07, 2015
Expiration Date: May 07, 2020

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Counterintelligence and Counterterrorism w/Change 1, May 28, 2015

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | AppendixA | AppendixB | AppendixC | ALL |

Chapter 1: Introduction

1.1 Overview

The NASA CI/CT Program is administered in accordance with the National Aeronautics and Space Act and in conformance with other applicable laws, EOs, PDDs, Federal regulations, to include NASA CI/CT Operating Instructions (OI), NPDs and NPRs, the MOU established with the FBI, and programmatic standards established by the National CI Executive, i.e., Defensive CI/CT programs. The OI and MOU provide additional and more specific guidance not included in this NPR due to the classified nature of the information. Responsibilities and procedures were developed to allow flexibility to mitigate Center-specific national security threats.

1.2 Organization

The NASA CI/CT Program is centrally managed by the OPS CI/CT Division, and the Division is administered locally at each of the NASA Field Centers. Headquarters staffing consists of the Director of CI/CT for Protective Services (DCI), Regional Program Managers and analysts who establish policy, provide centralized program management, and provide CI/CT support to Headquarters managers and employees. The CI/CT offices at the Field Centers and their associated support facilities are staffed by CISAs responsible for implementing the core CI/CT Program services, inquiries, and support to national security investigations.

1.3 Responsibilities

1.3.1. **The Assistant Administrator for Protective Services** (AA/OPS) will oversee Agency implementation, integration of, and compliance with CI/CT national security requirements by providing direction and ensuring that adequate resources are requested to accomplish CI/CT Program services. The AA/OPS shall also provide support to national security investigations in support of the overall NASA mission in accordance with NPD 1600.2, NASA Security Policy, and NPD 1600.4, National Security Programs.

1.3.1.1. The AA/OPS designates the DCI who is responsible for representing the NASA CI/CT Program at national-level meetings, as well as directing, managing, and developing policy and procedures for the program.

1.3.2. **The DCI** is responsible for all CI/CT program services, inquiries, support to national security investigations and cyber CI/CT occurring at NASA Headquarters, Field Centers, Component Facilities and Technical and Service Support Centers, and for coordinating those matters within NASA, the U.S. Intelligence Community (USIC), and other departments and agencies. The DCI shall:

a. Ensure the AA/OPS, the NASA Administrator, and key NASA senior executives are kept apprised of CI/CT national security matters impacting NASA. The DCI shall serve as NASA's senior subject-matter expert on CI/CT matters.

b. Prioritize CI/CT program objectives; identify resources, training and equipment needs; and supervise the CISAs assigned at Headquarters and Center CI/CT offices.

c. Oversee the implementation of CI/CT program policy and procedures and evaluate compliance in accordance with OPS and CI/CT Division policies.

d. Ensure NASA-related CI/CT national security matters are coordinated with the FBI. When reasonable belief suggests there may be a basis for an espionage or terrorism investigation, immediately refer the matter pursuant to section 811 of the Intelligence Authorization Act of 1995 [50 U.S.C. 402(a)]. Cooperation and contact with the FBI will be governed by the MOU between NASA and the FBI. The FBI assumes the role of lead investigative agency with CISA support and assistance.

e. Oversee the NASA CI Investigation Management System for CI/CT services, inquiries, and support to national security investigations. Authorize the initiation and closure of all NASA CI/CT threat assessments and preliminary inquiries and CI/CT national security investigations supported by CISAs. This approval authority is also delegated to the Regional Program Managers.

f. Direct the Agency's CI/CT awareness and reporting program. Ensure CI/CT offices maintain outreach programs that foster NASA personnel awareness and reporting of espionage, insider threats, FIE, and activities related to domestic and international terrorism.

g. Maintain a defensive CI/CT foreign travel briefing and debriefing program for NASA personnel traveling on official NASA business to designated countries, Russia, and other high-threat locations as defined by the National Intelligence Priorities Framework (NIPF) or the Department of State's Security Environment Threat List (SETL).

h. Maintain a defensive CI/CT briefing and debriefing program for NASA personnel hosting and escorting foreign visitors and assignees from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.

i. Direct CI/CT support to NASA's Foreign National Access Management System (FNAMS) in accordance with NPR 1600.4, Identity and Credential Management. Ensure Headquarters and Center CISAs evaluate CI/CT risks of visits and assignments of foreign visitors and Lawful Permanent Residents (LPR) from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.

j. Coordinate with the OPS Intelligence Division to obtain CI/CT analytic support.

k. Direct CI/CT support to NASA's Insider Threat Program, as required by NPD 1600.9, NASA Insider Threat Program.

l. Direct and prioritize CI/CT support to NASA's major technology protection programs and special activities.

m. Direct and prioritize cyber CI/CT support to NASA's Information Security Program, which includes the Agency's Chief Information Officer (CIO), OCIO, IT Security (ITS) Division, Center Information Security Officers (CISO), and Security Operations Center (SOC) in accordance with NPD 2810.1, NASA Information Security Policy, and NPR 2810.1, Security of Information Technology:

(1) Direct cyber CI/CT inquiries and support national security investigations of NASA's cyber environment to identify hostile foreign intelligence cyber operations, Advanced Persistent Threats (APT), and terrorism and provide threat mitigation information to enhance NASA's overall IT security posture.

(2) Facilitate collaboration, reporting, and information sharing among the Agency's OCIO, ITS, CISO, SOC, OIG, law enforcement, USIC, and the National Cyber Investigative Joint Task Force on cyber CI/CT-related matters.

n. Coordinate CI/CT national security matters with the Office of International and Interagency Relations, Office of General Counsel, the NASA Export Control Program, and other key NASA programs and officials as necessary. Coordinate with the NASA OIG on matters of mutual concern, including cyber CI/CT and matters with potential criminal liability, in accordance with the MOU between the OIG and OPS, dated February 3, 2011, and NPD 1600.4, National Security Programs.

o. Manage and safeguard CI/CT program files and information maintained at Headquarters and Center CI/CT offices in accordance with NPR 1441.1, NASA Records Retention Schedules. Ensure CI/CT facilities meet security requirements for the use and storage of Classified National Security Information (CNSI) and establish procedural requirements that supplement requirements for the maintenance, retention, and disposition of classified information. While supplementary requirements concerning how to maintain and disposition classified records may be able to be set through other directives established by the CI/CT Program, changes to how long to retain the records shall follow the process(es) established in NPR 1441.1, which includes approval by the National Archives and Records Administration.

1.3.3. **CISAs at Headquarters and Center CI/CT offices shall:**

a. Ensure Headquarters senior managers, Center Directors, and Center Chiefs of Protective Services/Chiefs of Security (CCPS/CCS) are kept apprised of CI/CT national security matters impacting NASA personnel and facilities.

b. Serve as primary advisors to Headquarters senior managers, Center Directors, and CCPS/CCS on CI/CT-related matters.

c. Restrict access to sensitive CI/CT information and classified national security matters to individuals with proper clearances and a strict need to know.

d. Act as liaison and coordinate NASA CI/CT issues with the FBI, USIC, and other Federal, state, and local agencies.

e. Conduct CI/CT services and inquiries and support national security investigations in accordance with CI/CT Division policies, OIs, and the MOU between NASA and the FBI.

f. Maintain a localized CI/CT awareness and reporting program that includes:

(1) General and comprehensive CI/CT awareness briefings and training to NASA personnel. Topics shall include, but are not limited to, an overview of espionage indicators, Foreign Intelligence Entity (FIE), insider threats, terrorism, and NASA personnel reporting requirements;

(2) Refresher briefings designed to reinforce and update awareness of CI/CT issues and reporting responsibilities.

(3) Tailored CI/CT awareness briefings and training for site-specific personnel groups assigned to sensitive positions, programs, or special access programs.

(4) Procedures for reporting suspicious activities or allegations.

(5) Dissemination of CI/CT awareness and education products and materials.

g. Conduct defensive CI/CT foreign travel and foreign contact briefings and debriefings of NASA personnel traveling on official NASA business to designated countries, Russia, and other high-threat locations as defined by the NIPF or SETL in accordance with NPR 9700.1, Travel. Travel and foreign contact briefings and debriefings may be extended to include personnel traveling to international or U.S.-based conferences, symposiums, and workshops where personnel may be exposed to potential CI/CT threats. This includes travel to non-designated countries, or low-threat locations, which involve meeting with foreign nationals from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.

h. Conduct defensive CI briefings and debriefings of NASA personnel hosting and escorting foreign visitors and assignees from designated countries, Russia, and other high-threat locations as defined in the NIPF or SETL, to include those NASA personnel who maintain close and continuous contact with any foreign national outside official duties.

i. Provide CI/CT support to NASA's FNAMS:

(1) Evaluate visits and assignments of foreign visitors and LPRs from designated countries, Russia, and other high-threat locations as defined by the NIPF or SETL to assess CI/CT threats. Assessments may also be extended to any foreign visitor, regardless of country status, who will be conducting NASA work that permits access to sensitive NASA information, technologies, or security areas.

(2) Provide CI/CT consultation and evaluate foreign national access for the NASA facility foreign national visit approval authority.

j. Provide CI/CT support to Agency and Center-specific technology protection programs, which includes the Office of Chief Technologist, Office of Chief Engineer, Office of Chief Scientist, Office of Chief Information Officer (OCIO), NASA's Technology Transfer Program, Research and Technology Program, Export Control Program, Office of Protective Services, and Space Asset Protection Program in support of NASA Space Flight programs and projects pursuant to NPR 1600.1, NASA Security Program Procedural Requirements; NPD 1600.2, NASA Security Policy; NPR 7120.5, NASA Space Flight Program and Project Management Requirements; NPR 1080.1, Requirements for the Conduct of NASA Research and Technologies; and NPR 7500.2, NASA Technology Transfer Requirements.

k. Provide cyber CI/CT support to Agency and Center-specific Information Security Programs, which includes the OCIO, ITS, CISO, and SOC.

l. Maintain collaborative and reciprocal relationships with NASA OIG offices and coordinate matters of mutual concern, including cyber CI/CT and matters with potential criminal liability, in accordance with the MOU between the OIG and OPS, dated February 3, 2011, and NPD 1600.4, National Security Programs.

m. Provide CI/CT support to NASA's Insider Threat Program.

n. Manage and safeguard CI office files and national security investigation records in accordance with CI/CT program policy and NASA records management and retention schedules.

1.3.4. **Headquarters Managers and Center Directors shall:**

a. Provide suitable office space (e.g., furniture, small conference area, and IT communication support services) for assigned CISAs to operate in a secure and mission-effective environment.

b. Ensure that all information or allegations of actual or suspected espionage or terrorism received by management are reported to the servicing CI/CT office.

c. Direct NASA personnel under their control to comply with the responsibilities under this NPR.

d. Direct NASA personnel under their control to cooperate fully in the conduct of CI/CT inquiries and national security investigations and make available all relevant NASA files (electronic and paper), documents, premises, and employees; except as limited by law; including access to records, premises, and employees through any access provision governing NASA's arrangement with third parties (e.g., contract access clauses).

e. Direct NASA program/project managers under their control to consider CI/CT support and integration in their pre-project planning, acquisition, and functional activity phases to ensure protection of NASA technology programs and activities, as required by NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

1.3.5. **All NASA Personnel (Civil Service and Contractor)** are required to protect CNSI, Export Controlled/Export Administrative Regulations (EAR), International Trafficking in Arms Regulations (ITAR), NASA Critical Information (NCI), SBU/CUI, proprietary, trade secret, and dual-use (commercial and military application) technologies affecting U.S. national and economic security in accordance with NPR 1600.1, NASA Security Program Procedural Requirements; NPR 1600.2, NASA Classified National Security Information; EO 13556, November 4, 2010, Implement Controlled Unclassified Information; NID 1600.55, Sensitive But Unclassified (SBU) Information; and PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts. This does not preclude other reporting requirements cited in NPR 1600.1, NASA Security Program Procedural Requirements, and NPR 1600.2, NASA Classified National Security Information. Accordingly, all NASA personnel shall:

a. Report to their servicing CI/CT office any incidents of actual or suspected loss or compromise of CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), Communications Security (COMSEC) Material and Devices, and information regarding National Security Systems (NSS).

b. Report to their servicing CI/CT office any unusual or suspicious overtures by foreign nationals or representatives of a foreign entity to acquire NASA information outside established official channels, whether or not the information is CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), COMSEC Material and Devices, and information regarding NSS according to NPR 7500.2, NASA Technology Transfer Requirements.

c. Report to their servicing CI/CT office any information regarding suspected or actual threats related to espionage or terrorism.

d. Refrain from discussing the details of any CI/CT matter under investigation to anyone not involved in the official investigative process unless authorized by a CISA.

e. Contact their servicing CI/CT office to receive an in-person CI threat briefing prior to hosting or escorting a foreign visitor and participate in a debriefing upon completion of a visit from a designated country, Russia, or other high-threat location as defined in the NIPF or SETL. Visits include meetings that are held outside NASA-controlled facilities.

f. Contact their servicing CI/CT office to receive an in-person CI/CT foreign travel briefing prior to conducting official travel to a designated country, Russia, and other high-threat locations, as defined in the NIPF or SETL. NASA civil service personnel traveling to a non-designated country shall complete an electronic briefing and debriefing e-mailed to them by the CI/CT Safeguards Foreign Travel System. All personnel can request a CI/CT travel briefing for non-official/personal travel, regardless of destination, by contacting their servicing CI/CT office. Immediately upon return from travel, report any suspected security or CI/CT incidents encountered during travel to their servicing CI/CT office. Sensitive Compartmented Information cleared personnel conducting foreign travel must contact their servicing CI/CT office to receive a CI/CT focused foreign travel threat briefing prior to departure. Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel.

g. Cooperate fully with CISAs during CI/CT inquiries and national security investigations; and, following verification of access authorization, make available all relevant NASA files (electronic and paper), documents, premises, and employees; except as limited by law; including access to records, premises, and employees through any access provision governing NASA's arrangement with third parties (e.g., contract access clauses).

1.3.6. **NASA Mission Directorates, Mission Support Offices, Program and Project Managers** are responsible for the protection of NASA personnel and resources as specified by NPR 7120.5, NASA Space Flight Program and Project Management Requirements; NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; and NPR 7120.8, NASA Research and Technology Program and Project Management Requirements. Accordingly, Mission Directorates, Mission Support Offices, Program/Project Managers shall:

a. Provide CISAs access to relevant program/project information and personnel to assist in establishing and providing the proper level of CI/CT support to a sensitive program/project or NASA NCI.

b. Notify CISAs of any incidents, events, or circumstances of actual or suspected loss or compromise of CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), COMSEC Material and Devices, and information regarding NSS in accordance with NPR 7500.2, NASA Technology Transfer Requirements. This does not preclude other reporting requirements cited in NPR 1600.1, NASA Security Program Procedural Requirements, and NPR 1600.2, NASA Classified National Security Information.

c. Notify CISAs of any occurrences of unusual or suspicious contact between NASA personnel and foreign nationals.

d. Direct program/project managers and their personnel that are working on projects with foreign nationals or foreign entities (including space agencies, universities, private companies, and individuals) to receive a tailored foreign intelligence country threat briefing from their servicing CI/CT office prior to beginning the project and on an annual basis. Require managers to track personnel attendance at these briefings by name and the date training was completed.

| TOC | ChangeHistory | Preface | Chapter1 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS